VOL.1 NO.1 2011 - ISSN 2088-6519

The 1st SEMNASTIK MTI

Seminar Nasional Teknologi Informasi & Komunikasi

Palembang - Indonesia

PROSIDING

Magister Teknik Informatika
Program Pascasarjana
Universitas Bina Darma

Universitas Bina Darma

APTIKOM

CISCO

NIIT

DEWAN REDAKSI PROSIDING SEMNASTIK
PROGRAM PASCASARJANA UNIVERSITAS BINA DARMA

SAMBUTAN DIREKTUR

Puji syukur kita sampaikan ke hadirat ALLAH SWT atas rahmat dan karuniaNya kita telah dapat menghasilkan sebuah dokumen akademik dari lingkungan Program Pascasarjana Universitas Bina Darma yang sangat monumental ini.

Pelaksanaan seminar dan diseminasi di lingkungan Universitas sesungguhnya merupakan bagian dari tugas pokok akademiknya sebagai wujud akhir pelaksanaan darma penelitian.

Oleh karenyanya, melalui penerbitan prosiding seminar nasional teknologi informasi dan komunikasi Ini, Saya sangat menghargai dan menyambut dengan antusias kerja keras segenap staff Program Studi Magister Teknik Informatika.

Semoga dengan keberhasilan penyelenggaraan program seminar secara berkala yang dilanjutkan dengan penerbitan prosiding sebagai dokumen/naskah akademik, atmosfir akademik di lingkungan Program Pascasarjana akan semakin baik dan meningkat. Semoga ALLAH SWT meridhoi usaha kita bersama.

Palembang, 1 Juli 2011

M. Izman Herdiansyah, PhD

ANALISA PENERAPAN IDS DAN IPS DALAM KEAMANAN JARINGAN KOMPUTER

Johansyah Al Rasyid [1], M. Izman Herdiansyah [2], Dedy Syamsuar [3]
[1] Teknik Elektronika, Politeknik Negri Srwijaya
[2,3] Magister Teknik Informatika, Universitas Bina Darma
email: johansyah_alrasyid@yahoo.com[1], herdians1816@gmail.com[2], dsyamsuar@mail.binadarma.ac.id[3]

ABSTRAK

Jaringan komputer yang terhubung ke internet membutuhkan sistem keamanan dari gangguan hacker yang melakukan penyusupan yang bertujuan melakukan tindakan tidak terpuji.. Solusi keamanan tersebut dengan menggunakan sistem pendeteksi penyusupan (IDS) dan sistem pencegah penyusupan (IPS). IDS akan mendeteksi jika ada penyusupan dan IPS akan melakukan pencegahan penyusupan. Dengan penggunaan keduanya, jaringan komputer lebih aman dari penyusupan.

Kata Kunci: Internet, hacker, IDS, IPS.

I. PENDAHULUAN

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya di satu sisi mempermudah pekerjaan-pekerjaan manusia sehari-hari, di sisi lain timbul masalah yang sangat serius, yakni aspek keamanan. Aspek keamanan perlu mendapat perhatian yang sangat serius karena manusia sangat tergantung dengan sistem informasi sehingga insiden keamanan meningkat tajam tiap tahun.

Kepedulian terhadap keamanan sistem informasi masih sangat kurang. Untuk mengatasinya dilakukan langkah-langkah preventif baik secara teknik yaitu *hardening* di sistem operasi, aplikasi, infrastruktur jaringan, implementasi sistem pendeteksi dan pencegahan penyusupan. Dan secara non teknik yaitu membuat *security policy* yang baik dan terkendali.

Jaringan komputer, seperti *Local Area Network (LAN)* dan Internet, memungkinkan untuk menyediakan informasi secara cepat. Ini salah satu alasan perusahaan atau organisasi mulai membangun-bondong membuat *LAN* untuk sistem informasinya dan menghubungkan *LAN* tersebut ke Internet. Terhubungnya *LAN* atau komputer ke Internet membuka potensi adanya lubang keamanan (*security hole*) yang tadinya bisa ditutupi dengan mengontrol keamanan secara fisik. Ini sesuai dengan pendapat bahwa kemudahan (kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri. Semakin tinggi tingkat keamanan, semakin sulit (tidak nyaman) untuk mengakses informasi.

Intrusion Detection System (IDS) atau Sistem Deteksi Penyusup adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusup. *IDS* akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. *IDS* tidak melakukan pencegahan terjadinya penyusup. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana melakukan konfigurasi *IDS*. Pada saat terjadi penyusupan ke sistem jaringan komputer sering kali administrator tidak berada di tempat (lokasi *server* sistem jaringan) sehingga penyusup yang masuk tidak segera dapat diketahui, dihalangi dan diantisipasi (*counter*). Hal ini pada akhirnya menyebabkan sistem jaringan dapat ditembus penyusup sehingga dapat menimbulkan kerugian yang besar pada pengguna sistem jaringan.

Untuk mengatasi permasalah tersebut, diperlukan sebuah sistem yang berfungsi untuk melaksanakan suatu pencegahan terhadap penyusupan yang terjadi pada jaringan komputer. *Intrusion Prevention System (IPS)* atau sistem pencegahan penyusupan adalah sistem komputer (berupa *Software*) yang berusaha melakukan pencegahan terhadap penyusupan. *IPS* akan melakukan pencegahan terhadap suatu tindakan illegal yang terjadi dalam jaringan komputer. Pencegahan yang dilakukan berdasarkan konfigurasi *IPS* yang diterapkan. Dengan penerapan *IPS*, penyusupan yang terjadi di jaringan komputer dapat ditanggulangi dengan cepat sehingga tidak terjadi kerusakan pada sistem walaupun administrator tidak berada di tempat.

ISSN 2088-6519

2 TINJAUAN PUSTAKA

2.1 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) atau sistem deteksi penyusup adalah sistem komputer (bisa merupakan kombinasi *software* dan *hardware*) yang berusaha melakukan deteksi penyusupan. IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi IDS.(Wikipedia Indonesia, 2010)

2.1.1 Jenis-Jenis IDS

Ada dua jenis IDS, yakni: *Network-based Intrusion Detection System* (NIDS): Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana server berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan *switch Ethernet*, meskipun beberapa *vendor switch Ethernet* sekarang telah menerapkan fungsi IDS di dalam *switch* buatannya untuk memonitor port atau koneksi.

*Host-based Intrusion D*etection System (HIDS): Aktivitas sebuah host jaringan individual akan dipantau apakah terjadi sebuah percobaan serangan atau penyusupan ke dalamnya atau tidak. HIDS seringnya diletakkan pada server-server kritis di jaringan, seperti halnya *firewall,* web server, atau server yang terkoneksi ke Internet.

2.1.2 Metoda Kerja IDS

Tiga metoda yang digunakan IDS dalam mendeteksi penyusupan, yakni :

Pendeteksian berbasis *signature* (seperti halnya yang dilakukan oleh beberapa antivirus), yang melibatkan pencocokan lalu lintas jaringan dengan basis data yang berisi cara-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama seperti halnya antivirus, jenis ini membutuhkan pembaruan terhadap basis data signature IDS yang bersangkutan.

Pendeteksian adanya anomali, yang disebut sebagai *Anomaly-based IDS*. Jenis ini melibatkan pola lalu lintas yang mungkin merupakan sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya, dilakukan dengan menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan *signature-based IDS*, yakni ia dapat mendeteksi bentuk serangan yang baru dan belum terdapat di dalam basis data *signature* IDS. Kelemahannya, adalah jenis ini sering mengeluarkan pesan *false positive*. Sehingga tugas administrator menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan *false positive* yang muncul.

Pendeteksian dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, utamanya berkas log. Teknik ini seringnya diimplementasikan di dalam HIDS, selain tentunya melakukan pemindaian terhadap integritas sistem untuk memantau apakah terjadi kejadian yang tidak biasa.

2.2 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) adalah sebuah aplikasi yang bekerja untuk *monitoring* traffic jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap serangan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. Bisa jadi karena adanya serangan dari luar, dan sebagainya. Produk IPS sendiri dapat berupa perangkat keras (*hardware*) atau perangkat lunak (*software*). (Wikipedia Indonesia, 2010)

2.2.1 Jenis-jenis IPS

Ada dua jenis IPS, yaitu :*Host-based Intrusion Prevention System* (HIPS) adalah sama seperti halnya *Host-based Intrusion Detection System* (HIDS). Program agent HIPS diinstall secara langsung di sistem yang diproteksi untuk dimonitor aktifitas sistem internalnya. HIPS di binding dengan kernel sistem operasi dan services sistem operasi. Sehingga HIPS bisa memantau dan menghadang system call yang dicurigai dalam rangka mencegah terjadinya intrusi terhadap host. HIPS juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu. Sebagai contoh HIPS untuk mencegah intrusio pada webserver misalnya. Dari sisi security mungkin solusi HIPS bisa mencegah datangnya ancaman terhadap *host*. Tetapi dari sisi performance, harus diperhatikan apakah HIPS memberikan dampak negatif terhadap *performance host*. Karena menginstall dan binding HIPS pada sistem operasi mengakibatkan penggunaan resource komputer host menjadi semakin besar.

ISSN 2088-6519

Network-based Intrusion Prevention System (NIPS) tidak melakukan pantauan secara khusus di satu host saja. Tetapi melakukan pantauan dan proteksi dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan *firewall* dan sering disebut sebagai *In-Line IDS* atau *Gateway Intrusion Detection System* (GIDS).

Metoda Kerja IPS

Ada tiga metoda kerja IPS :Sistematika IPS yang berbasis *signature* adalah dengan cara mencocokkan lalu lintas jaringan dengan *signature* database milik IPS yang berisi *attacking rule* atau pola-cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Sama halnya dengan antivirus, IPS berbasis *signature* membutuhkan update terhadap *signature database* untuk metode-metode penyerangan terbaru. IPS berbasis *signature* juga melakukan pencegahan terhadap ancaman intrusi sesuai dengan *signature database* yang terlanggutan.

Sistematika IPS yang berbasis anomali adalah dengan cara melibatkan pola-pola lalu lintas jaringan yang pernah terjadi. Umumnya, dilakukan dengan menggunakan teknik statistik. Statistik tersebut mencakup perbandingan antara lalu lintas jaringan yang sedang di monitor dengan lalu lintas jaringan yang biasa terjadi (*state normal*). Metode ini dapat dikatakan lebih kaya dibandingkan *signature-based* IPS. Karena *anomaly-based* IPS dapat mendeteksi gangguan terhadap jaringan yang terbaru yang belum terdapat di dilaporkan. Sehingga tugas *Network Administrator* menjadi lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya laporan *false positive* yang muncul database IPS. Tetapi kelemahannya adalah potensi timbulnya *false positive*, yaitu pesan/log yang belum semestinya.

Teknik lain yang digunakan adalah dengan cara melakukan monitoring berkas-berkas sistem operasi pada *host*. IPS akan melihat apakah ada percobaan untuk mengubah beberapa berkas sistem operasi, contohnya berkas log. Teknik ini diimplementasikan dalam IPS jenis *Host-based Intrusion Prevention System*.

3 KESIMPULAN

Penerapan IDS dan IPS secara bersama dapat melaksanakan pengamanan jaringan komputer dari terjadinya penyusupan oleh hacker. Dimana IDS melaksanakan pendeteksian terhadap penyusupan yang terjadi di jaringan, dan memberikan peringatan akan adanya penyusupanSedangkan IPS melaksanakan pencegahan terhadap penyusupan yang terjadi di jaringan komputer. Kedua sistem ini bersinergi dalam melaksanakan keamanan jaringan terhadap penyusupan yang akan melakukan tindakan yang tidak baik

REFERENSI

[1] Deris Stiawan, *Intrusion Prevention System (IPS) dan Tantangan dalam Pengembangannya*, Fasilkom Unsri, Palembang, diakses 10 Oktober 2010

[2] IGN Mantra, *Desain Intruder Detection 'bv bv* 'diakses 10 Oktober 2010 diakses 10 Oktober 2010 *System(IDS) sebagai Antisipasi Hacker dan Cracker di Dunia Maya*, Proceeding pada Seminar Ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2008), ISSN : 1411-6286, diakses 10 Oktober 2010

[3] Krstoko Dwi Hartono, *Analisis Perancangan Perangkat Lunak Intrusion Detection System (IDS) pada Jaringan Komputer Berbasis Teknologi Mobile*, Seminar Nasional Sistem dan Informatika 2007, SNSI 07-050, diakses 10 Oktober 2010

[4] Puji Hartono, Sistem Pencegahan Penyusupan pada Jaringan berbasis Snort IDS dan IPTables Firewall, Tugas kuliah Keamanan Sistem Lanjut, 2006, diakses 10 Oktober 2010

[5] Wikipedia Indonesia, *Sistem Deteksi Intrusi*, diakses 10 Oktober 2010

[6] Wikipedia Indonesia, *Sistem Pencegah Intrusi*, diakses 10 Oktober 2010

ISSN 2088-6519